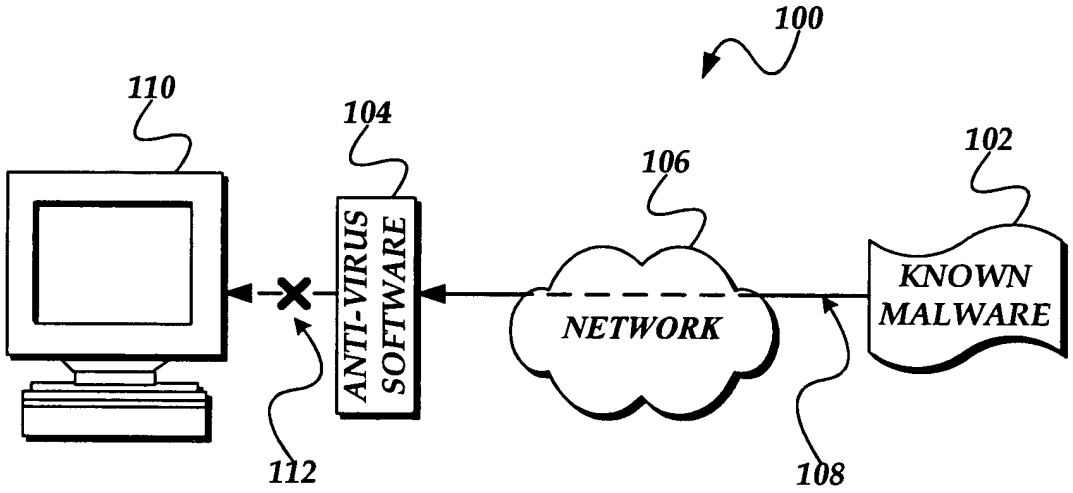

Fig.1A.

PRIOR ART

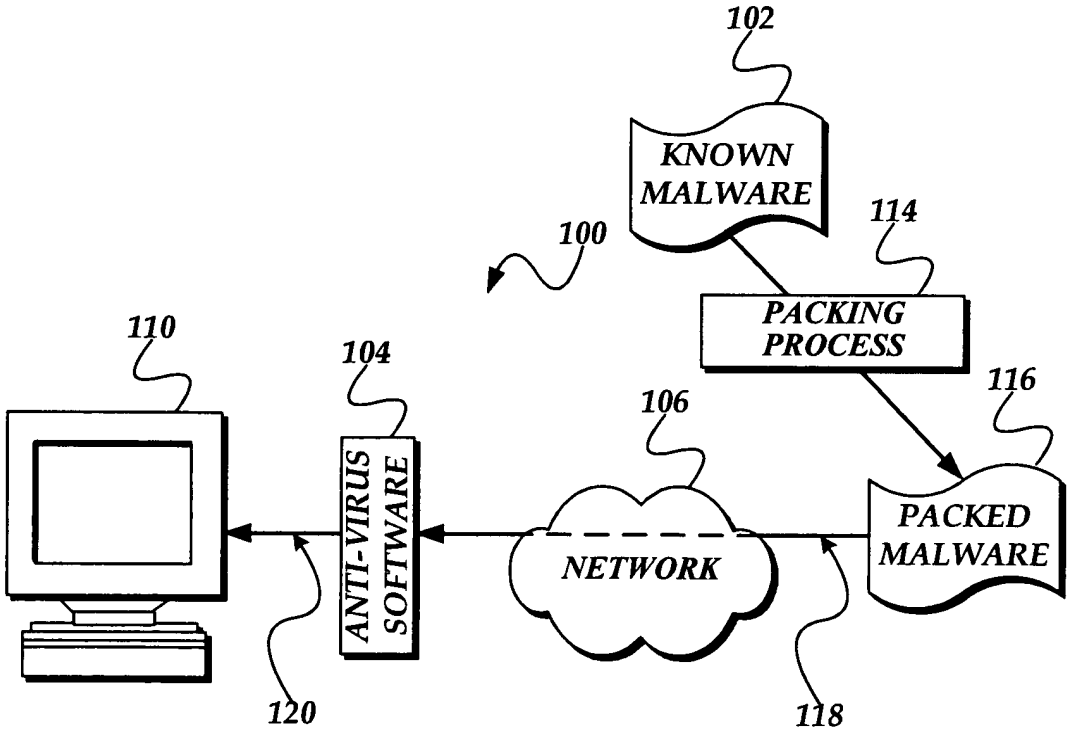

Fig.1B.

PRIOR ART

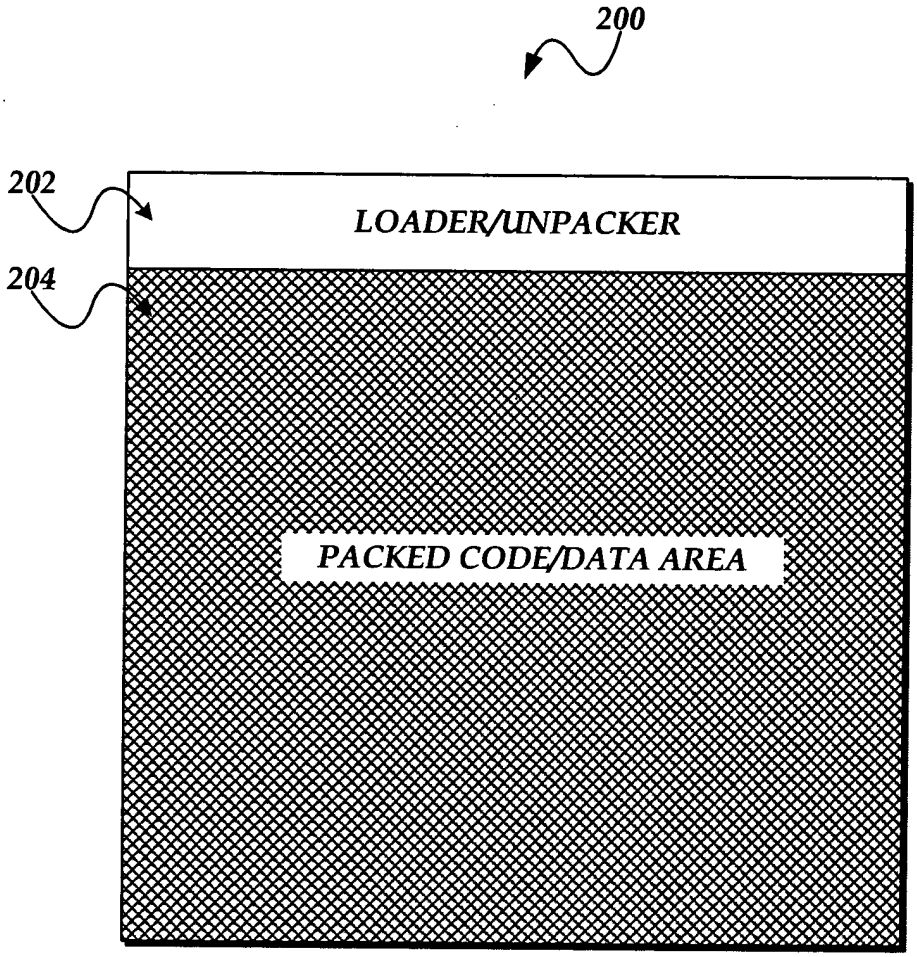

Fig.2.

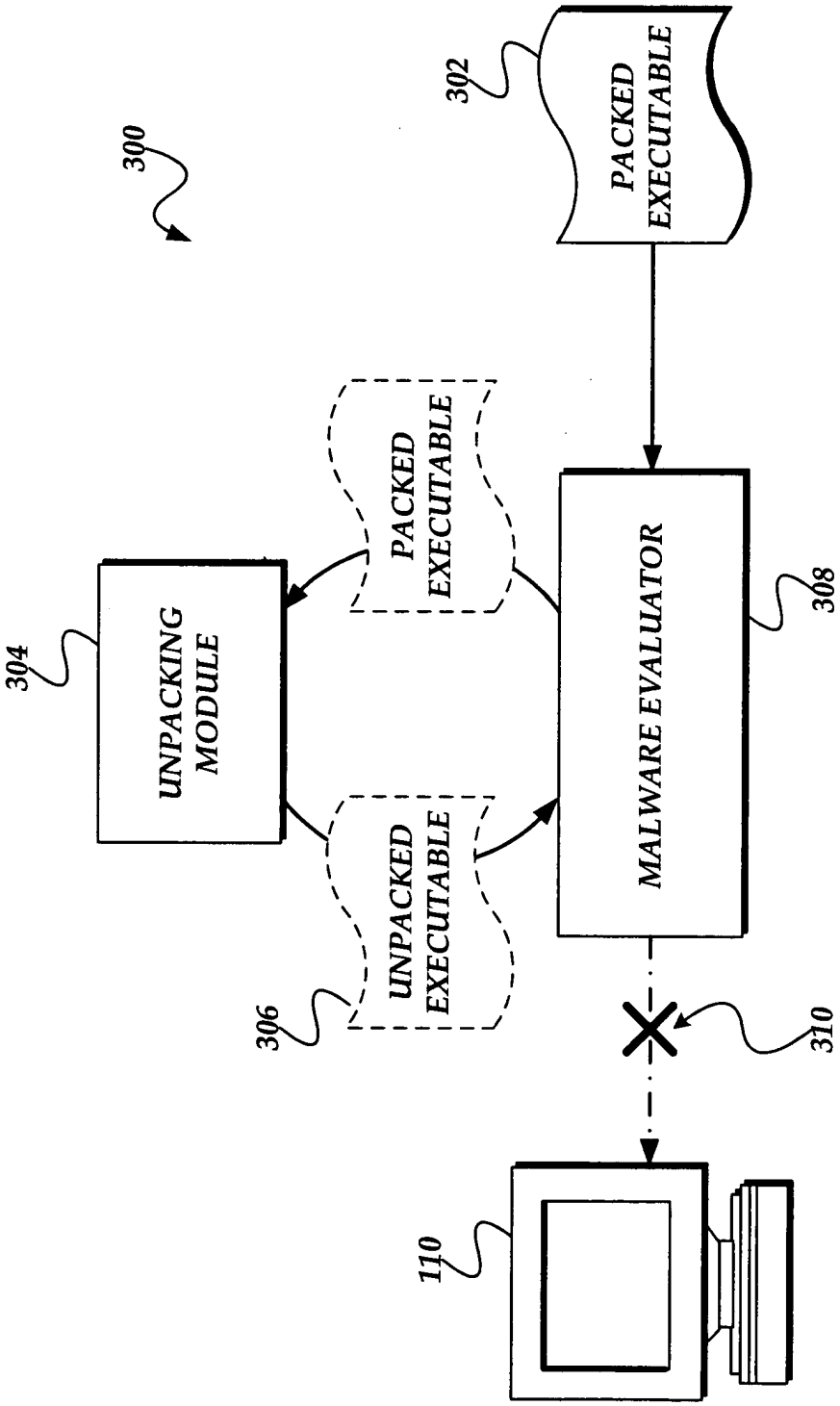
300
302
PACKED EXECUTABLE
PACKED EXECUTABLE
304
UNPACKING MODULE
306
UNPACKED EXECUTABLE
308
MALWARE EVALUATOR
310
110

Fig.3.

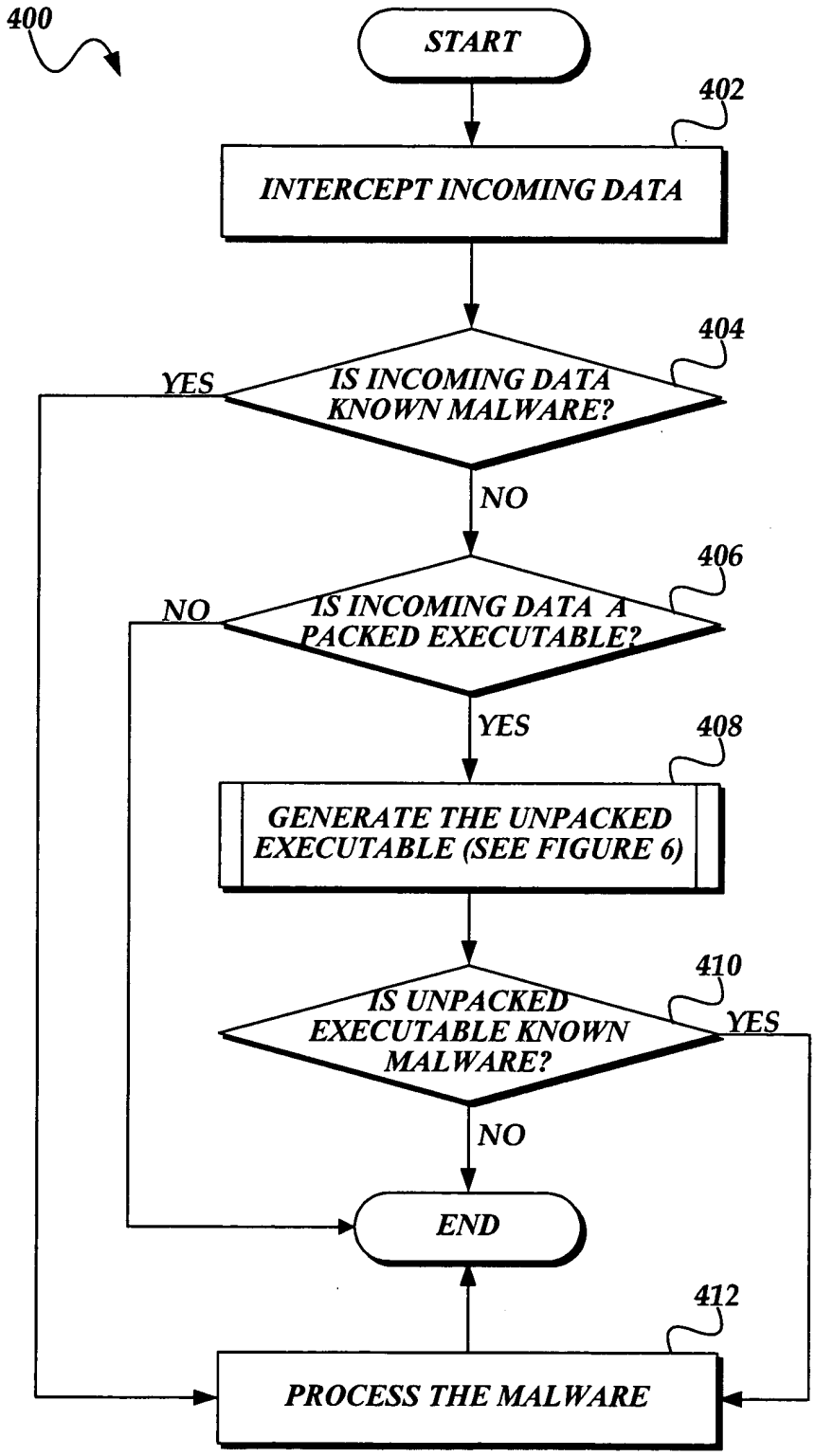
400
START
402
INTERCEPT INCOMING DATA
404
IS INCOMING DATA KNOWN MALWARE?
YES
NO
406
IS INCOMING DATA A PACKED EXECUTABLE?
NO
YES
408
GENERATE THE UNPACKED EXECUTABLE (SEE FIGURE 6)
410
IS UNPACKED EXECUTABLE KNOWN MALWARE?
YES
NO
END
412
PROCESS THE MALWARE

Fig.4A.

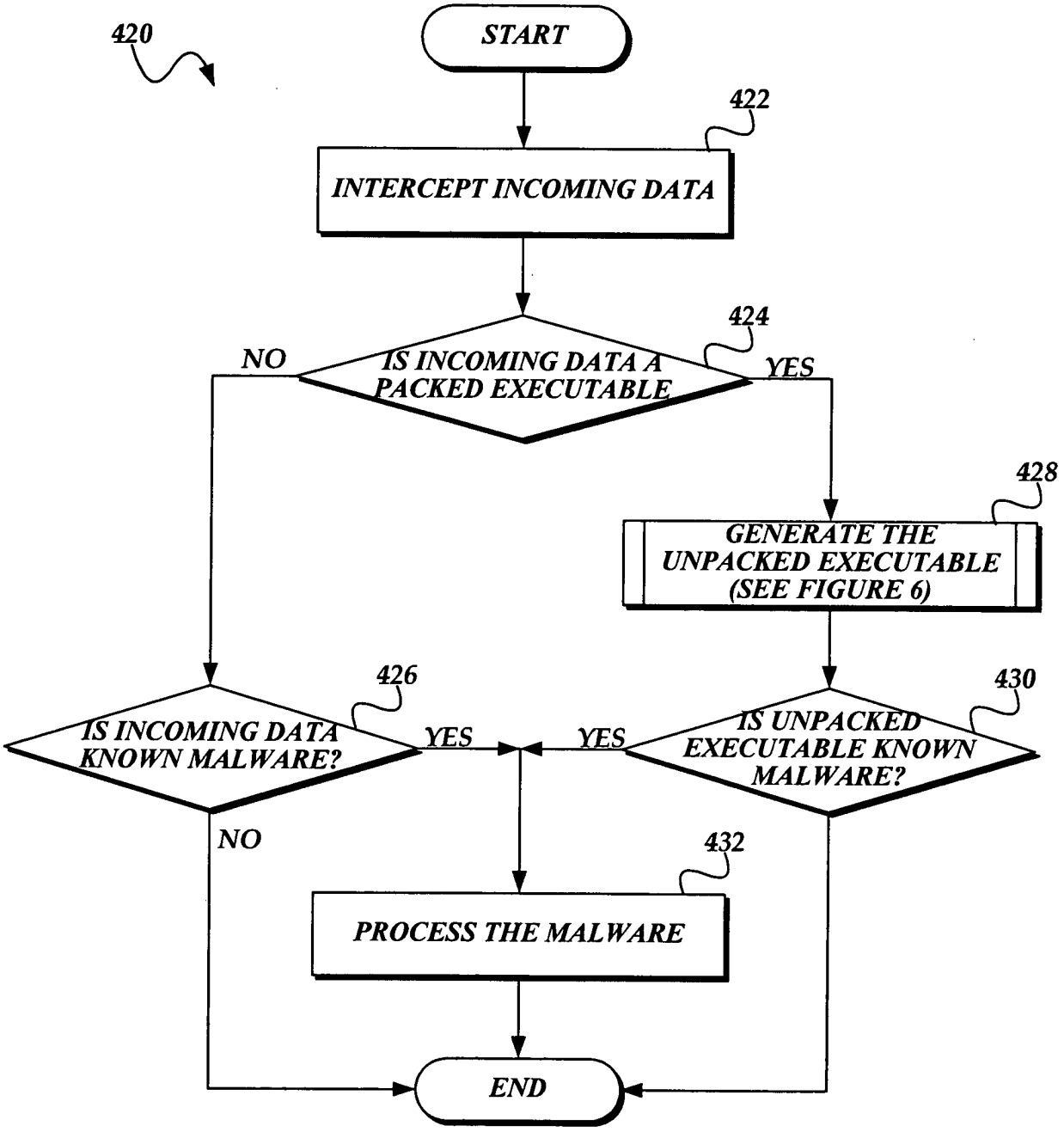
420
START
422
INTERCEPT INCOMING DATA
424
IS INCOMING DATA A PACKED EXECUTABLE
NO
YES
428
GENERATE THE UNPACKED EXECUTABLE (SEE FIGURE 6)
426
IS INCOMING DATA KNOWN MALWARE?
YES
YES
430
IS UNPACKED EXECUTABLE KNOWN MALWARE?
NO
432
PROCESS THE MALWARE
END

Fig.4B.

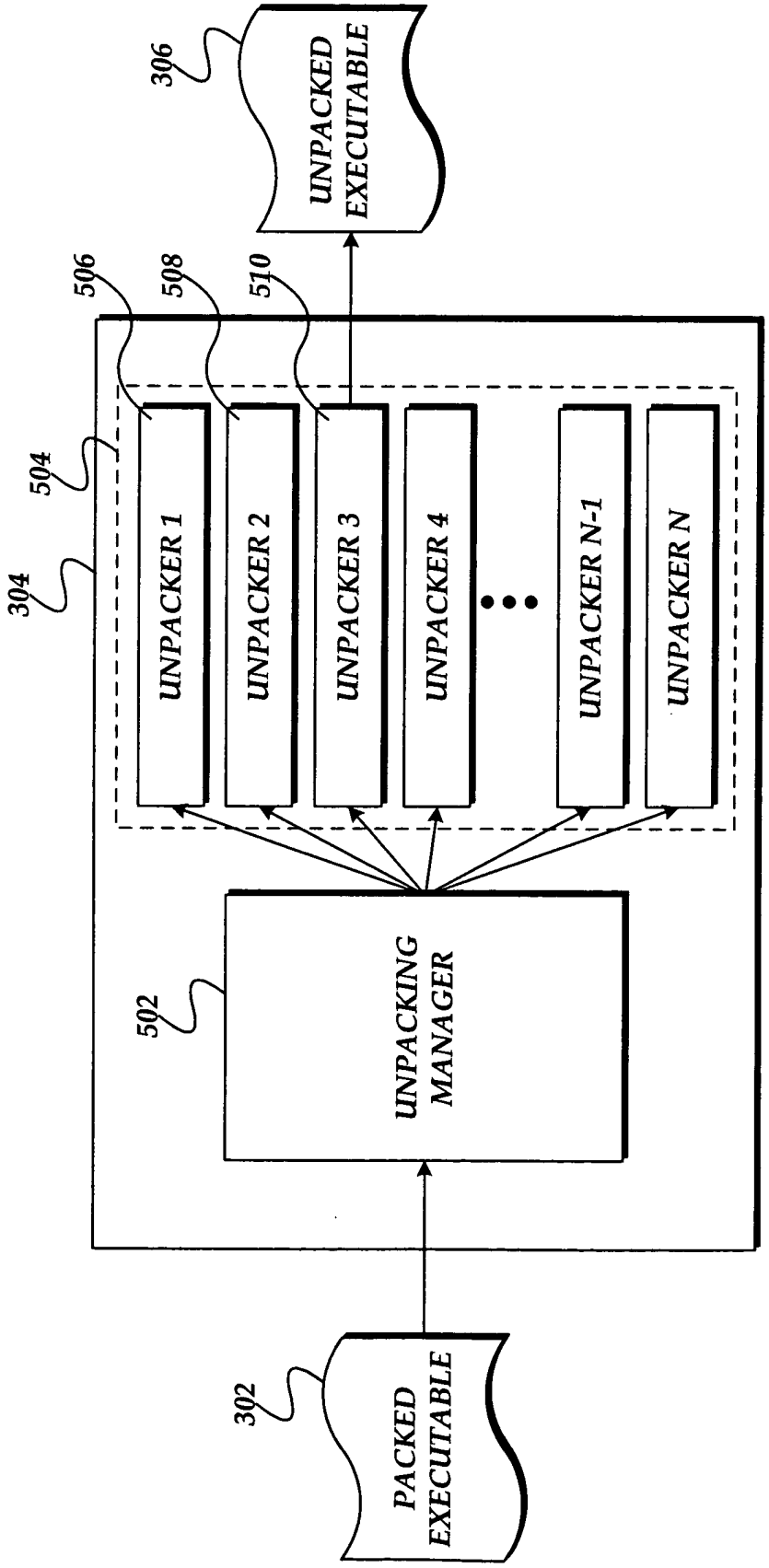
306
UNPACKED EXECUTABLE
506
508
510
504
304
UNPACKER 1
UNPACKER 2
UNPACKER 3
UNPACKER 4
UNPACKER N-1
UNPACKER N
502
UNPACKING MANAGER
302
PACKED EXECUTABLE

Fig.5.

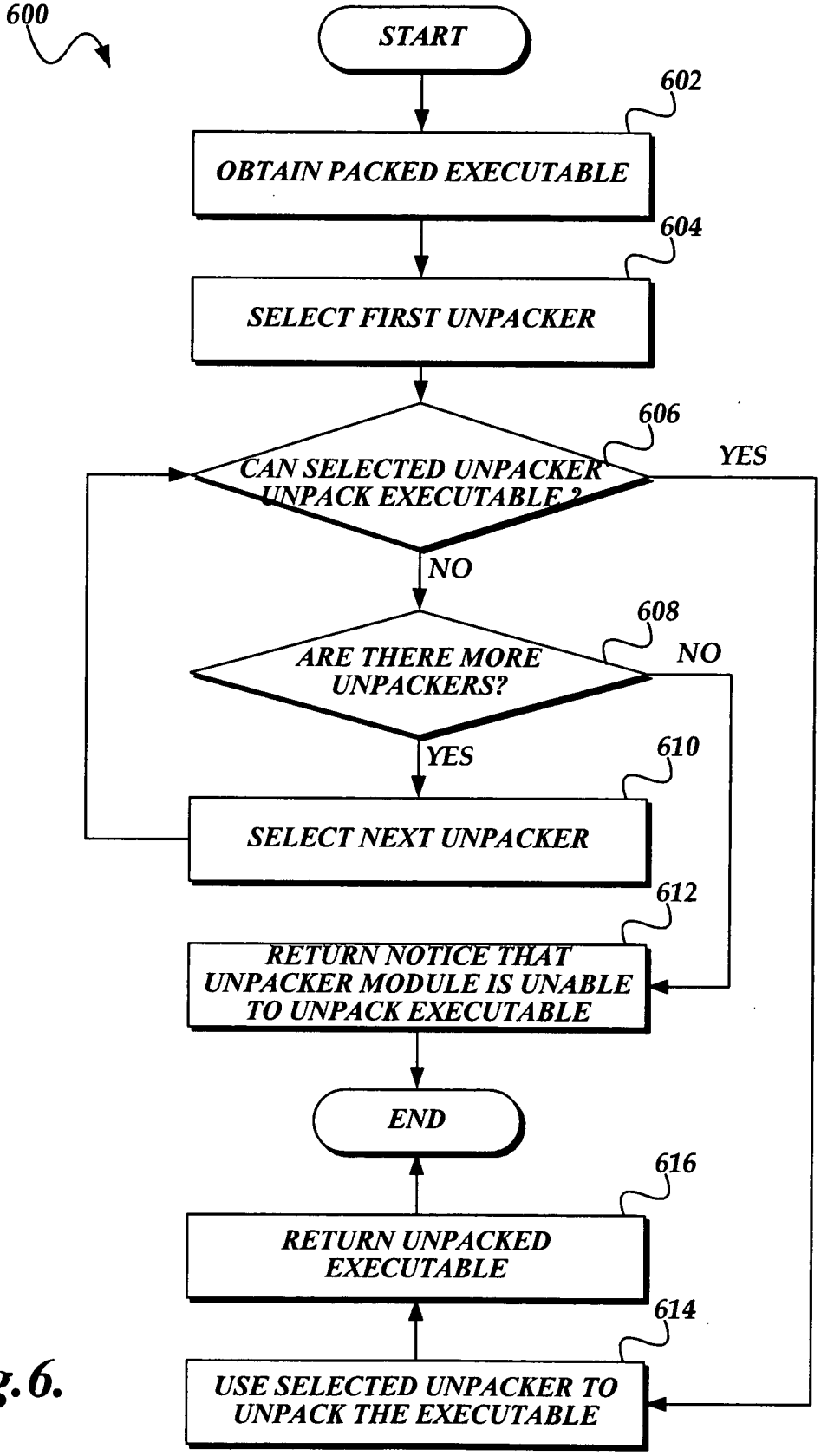
600
START
602
OBTAIN PACKED EXECUTABLE
604
SELECT FIRST UNPACKER
606
CAN SELECTED UNPACKER UNPACK EXECUTABLE ?
YES
NO
608
ARE THERE MORE UNPACKERS?
NO
YES
610
SELECT NEXT UNPACKER
612
RETURN NOTICE THAT UNPACKER MODULE IS UNABLE TO UNPACK EXECUTABLE
END
616
RETURN UNPACKED EXECUTABLE
614
USE SELECTED UNPACKER TO UNPACK THE EXECUTABLE

Fig. 6.

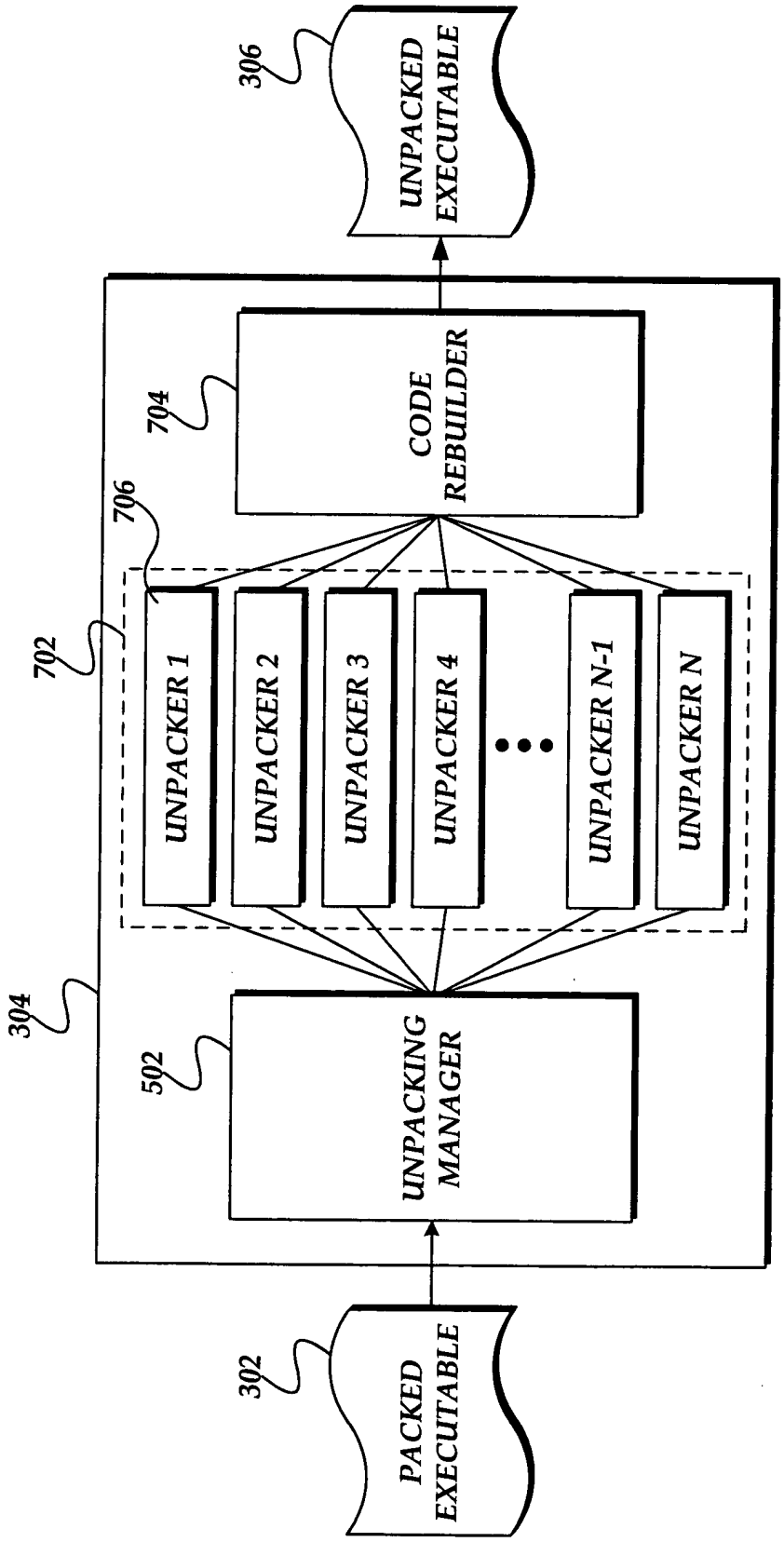
306
UNPACKED EXECUTABLE
704
CODE REBUILDER
706
702
UNPACKER 1
UNPACKER 2
UNPACKER 3
UNPACKER 4
UNPACKER N-1
UNPACKER N
304
502
UNPACKING MANAGER
302
PACKED EXECUTABLE

Fig. 7.